Tomasz DOMŻAŁ
Biuro Bezpieczeństwa Narodowego
W a r s z a w a

ZABEZPIECZENIE DANYCH W SYSTEMIE MONITOROWANIA PRZEWOZU ŁADUNKÓW NIEBEZPIECZNYCH

Przesyłanie i przechowywanie danych wymaga zabezpieczeń przed zagrożeniami o charakterze czynnym oraz biernym. W wyniku tych zagrożeń dane mogą być zmienione, bądź też dostęp do nich mogą uzyskać osoby nieuprawnione. Przeciwdziałanie temu wymaga uwzględnienia odpowiednich wymagań już na etapie opracowywania koncepcji i wstępnego projektu systemu. W pracy przedstawiono elementy metodyki projektowania i wdrożenia systemów z zabezpieczeniem danych.

ANALITYCZNE PODEJŚCIE DO PROJEKTOWANIA BEZPIECZNEGO SYSTEMU

Niniejsze opracowanie ma zwrócić uwagę na problematykę zabezpieczania przesyłu i magazynowania informacji (w systemie informatycznym) przed utratą danych, ich poufności i integralności.

Proces dochodzenia do skutecznie działającego systemu można podzielić na etapy:

1. Opracowanie strategii
   a) analiza potrzeb
   b) wybór zabezpieczeń systemu
   c) przegląd planu, uzgodnienia i konsultacje
2. Projektowanie inżynierskie
3. Instalacja, wdrażanie i szkolenie
4. Zarządzanie

Opracowanie strategii (PLAN)

Zasadniczymi kierunkami prac na tym etapie będą:

- określenie, jakie zasoby w omawianym systemie mają być chronione,
- kwalifikacja przesyłanych i magazynowanych informacji pod kątem ich poufności,
- określenie odpowiednich środków technicznych do obsługi (przesyłu i magazynowania) informacji o określonej klauzuli poufności.

Ponieważ każdy w/w punktów powinien być konsultowany w dalszych etapach z instytucjami odpowiedzialnymi za dystrybucję i ochronę dokumentów poufnych w omawianym systemie, należy już na etapie planowania określić jakie to będą instytucje, oraz zorganizować stałą współpracę z nimi. Instytucjami tymi będą np. Biuro Szyfrów Urzędu Ochrony Państwa oraz departamenty spraw obronnych lub prawne Min. Ochrony

Środowiska, Zasobów Naturalnych i Leśnictwa, Min. Przemysłu, Min. Łączności, Min. Gospodarki Morskiej i Transportu.
Ogólne zasoby omawianego systemu można podzielić na:
- informacje i dane,
- usługi komunikacyjne,
- urządzenia fizyczne, ośrodki, centra zarządzania i magazynowania informacji.

Możemy założyć, że w przypadku omawianego systemu monitorowania przewozu ładunków w skład zasobów będą wchodziły w szczególności elementy pokazane w tablicy 1.

Tablica 1. Informacje, usługi i zasoby fizyczne systemu monitorowania

Informacje o:	Usługi komunikacyjne	Zasoby fizyczne
- nadawcy transportu - odbiorcy - marszrucie (planowanej trasie przejazdu - ładunku (rodzaju i ilości) - środku transportowym - pozycji transportu - zdarzeniach nadzwyczajnych	- satelitarne - radiowe - telefoniczne - X.25 - PSTN - ATM? - poczta (X 400)	- centra komputerowe - urządzenia nadawczo-odbiorcze mobilne - urządzenia nadawczo-odbiorcze stacjonarne - urządzenia i fizyczne kanały transmisyjne (routery, krotnice, nadajniki)

* Wymienione tutaj pozycje nie wyczerpują wszystkich elementów systemu, np. nie są wymienione zasoby służb ratowniczych.

W/w lista zasobów informacyjnych zawiera pozycje, które mogą być jawne, ale też i takie, które powinny być chronione. Klasyfikację poufności i wagi informacji, w odniesieniu do konkretnych przypadków, powinni przeprowadzić specjaliści z Ministerstwa Przemysłu i Handlu i Ministerstwa Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa, we współpracy ze służbami ratowniczymi.
Rozważmy zagrożenia jakie mogą wystąpić dla w/w kategorii zasobów informatycznych:
- zagrożenia bierne, które ujawniają informację nie wpływają na jej zawartość.
- zagrożenia aktywne, które wpływają na autentyczność informacji i integralność baz.

Przed doborem odpowiednich środków ochrony, a po określeniu wagi przesyłanej informacji należy określić, kto informacje te będzie próbował pozyskać, zmienić lub zniszczyć, jakimi środkami może dysponować i jaki będzie koszt pozyskania tej informacji. Określmy zatem potencjalnych przeciwników. Może to być np. poniższa tabela:
1. hobbiści hackerzy;
2. osoby zainteresowane materialnie w uzyskaniu informacji;
3. zorganizowane grupy przestępcze;

4. grupy terrorystyczne;
5. obce służby specjalne.

Określenie, które z wymienionych kategorii przeciwników są dla systemu niebezpieczne, wymaga dokonania poważnej analizy, z uzwględnianiem rodzaju przesyłanej informacji.

Należy tutaj zauważyć, że o ile dość dokładnie można określić potencjał, jakim mogą dysponować pierwsze cztery grupy przeciwników, to trudno jest określić możliwości techniczne grupy piątej przy założeniu, że przeciwnik dysponuje dużymi możliwościami finansowymi. Musimy zatem przyjąć, że dokumenty o istotnym znaczeniu dla bezpieczeństwa państwa nie będą się pojawiały w słabych pod względem ochrony elementach systemu. Elementami takimi będą np. linie transmisyjne i nie chronione przed emisją komputery i monitory.

Zwrócić tutaj trzeba uwagę na "kierunki" ataku:
- ataki wewnętrzne,
- ataki zewnętrzne ze wspomaganiem wewnętrznym,
- ataki zewnętrzne.

Ocenia się, że w ponad 80% przypadków utrata poufności lub integralności informacji nastąpiła na skutek umyślnej lub nieumyślnej działalnością pracowników danej instytucji. Pozostałe przypadki udanych ataków zewnętrznych w znakomitej większości spowodowane były używaniem prostych haseł użytkowników i administratorów systemu oraz zbyt dużymi tolerancjami systemu na próby włamania. Ilustruje to wagę elementu organizacyjnego w systemie zabezpieczania danych. W instytucji, w której dostęp do informacji poufnych ma wiele osób o różnych uprawnieniach, muszą być ściśle określone zasady dostępu, wymuszane zmiany haseł i prowadzona kontrola dostępu (auditing).

Tablica 2.

	Przypadkowe	Umyślne (ataki)
Bierne	- przesłuchy -utrata dokumentacji - nieostrożność obsługi	- podsłuch - kradzież - monitorowanie ruchu - ujawnianie informacji - ujawnianie haseł
Czynne	- błędy w oprogramowaniu - złe funkcjonowanie systemu - błędy obsługi	- wirusy - modyfikacje lub fałszowanie - zmiana tablic routingu przez nieuprawnionego użytkownika - przerwanie usług - zniszczenie informacji lub jej nośników

Projekt techniczny

Końcowym etapem procesu projektowania będzie dobór środków zabezpieczających. Nie ma tutaj miejsca na robienie przeglądu wszystkich możliwych zabezpieczeń, jednakże

chciałbym zwrócić uwagę na parę metod zabezpieczenia, które, po dokonaniu analizy omówionej poprzednio, mogą znaleźć zastosowanie.
Ogólnie mechanizmy zabezpieczeń możemy podzielić na 3 nierozłączne klasy:
1. Zapobieganie zagrożeniom.
2. Wykrywanie ataków.
3. Odtwarzanie po atakach lub zniszczeniach przypadkowych.

Ze względu na obszerność tematu wymieńmy tutaj tylko mechanizmy zabezpieczenia dla środowiska przesyłania danych (norma ISO 7498):
- kryptografia i szyfrowanie,
- zarządzanie kluczami,
- kontrola dostępu,
- podpis cyfrowy,
- kontrola integralności danych (modyfikacji strumienia informacji),
- wymiana legalizacji (upewnienie się co do autentyczności korespondenta),
- wypełnianie ruchu (generowanie ruchu pozorowanego),
- zarządzanie routingiem (wyznaczanie tras przebiegu komunikatu),
- notaryzacja (potwierdzanie wiarygodności korespondenta przez trzecią stronę),
- zabezpieczenia fizyczne i personalne,
- wiarygodny i sprawdzony sprzęt oraz oprogramowanie.

Oczywiście nie wszystkie z tych mechanizmów będą stosowane; wymienione zostały tutaj, ponieważ określa je norma ISO, która została już opublikowana przez PKN.

Mechanizmami, które muszą być stosowane w każdym systemie rozległym, przesyłającym informacje poufne jest szyfrowanie, zarządzanie kluczami i kontrola dostępu.

Istnieje wiele metod szyfrowania i zarządzania kluczami, opartych zarówno na rozwiązaniach sprzętowych, jak i programowych. Stosuje się zarówno algorytmy specyficzne dla danego produktu, jak i publikowane (np. DES czy RSA).

W 1977 roku Narodowe Biuro Normalizacji wprowadziło Standard Szyfrowania Danych DES (Data Encryption Standard) - permutacyjno-podstawieniowy symetryczny algorytm szyfrujący, oparty na 56-bitowym kluczu. Algorytm ten jest bardzo często stosowany do dnia dzisiejszego. W 1980 roku amerykańscy matematycy wykazali, że złamanie tego szyfru na specjalizowanej maszynie kosztującej wówczas 50 mln USD, przy ataku z tekstem jawnym trwałoby 2 dni (Denning "Cryptography & Data Security"). Przyjmując 100-krotny spadek cen można ocenić, że czas złamania klucza na maszynie wartej 1 mln USD dzisiaj wynosiłby 1 dzień, co przy założonym czasie amortyzacji 5 lat daje nam koszt jednego rozwiązania zaledwie 500 USD, a przy zastosowaniu rozwiązań z dużymi pamięciami magnetycznymi rzędu 10 TB koszt 1 rozwiązania mógłby spaść do 1 USD. Wyliczenia te świadczą, że algorytmy te zabezpieczają przed atakami ze strony hackerów, czy nawet, bardzo dobrze wyposażonymi grupami przestępczymi, jednak nie chronią przed specjalizowanymi służbami wywiadowczymi.

Innym ciekawym algorytmem stosowanym przede wszystkim do dystrybucji kluczy jest opublikowany w 1978 roku _ algorytm klucza publicznego. Algorytm ten ma znacznie większą moc kryptograficzną, jednakże nie nadaje się do szyfrowania dużej ilości danych.

W systemie docelowym powinno używać się różnych metod szyfrowania, zarówno sprzętowych jak i programowych a także różnych algorytmów do szyfrowania danych i zarządzania kluczami.

Szkolenie, zarządzanie, kontrola dostępu

Najsłabszym ogniwem w systemie jest zwykle człowiek. Nawet największe zabezpieczenia nie wystarczą, jeżeli nie będą przestrzegane zasady ochrony systemu. Wspomniane w po-przednim punkcie szacowania kosztów włamania do system dotyczyły metod tzw. "brutalnych". Hackerzy takich metod nie stosują. Hasła są ujawniane zwykle na skutek niestosowania podstawowych zasad bezpieczeństwa przez personej firmy. Np. badania ekspertów od zabezpieczeń systemów bankowych w Stanach Zjednoczonych wykazały, że 60% haseł to po prostu nazwa firmy ewentualnie z niewielkimi modyfikacjami, popularne imiona (zwykle małżonków i dzieci pracownika), lub nazwiska modnych w danej chwili aktorów i sportowców.

Dlatego też niezmiernie ważnym elementem bezpieczeństwa jest opracowanie szczegółowych reguł postępowania w zakresie utrzymania poufności i autentyczności danych, szkolenie personelu oraz regularny dostęp (auditing).

W przypadku większych systemów powinna być wyznaczona osoba (security officer), lub zespół podległy bezpośrednio kierownictwu firmy, kontrolujący na bieżąco stan zabepieczenia systemu i prawidłowość jego obsługi.